The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 29

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte YUSUKE SHIMIZU, YOICHI UCHIDA, and SEIJI ADACHI

Appeal No. 2002-1658
Application No. 08/922,339

HEARD: May 8, 2003

Before HAIRSTON, KRASS, and GROSS, Administrative Patent Judges.
GROSS, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 4 through 11, 13, 15 through 22, 25, 27, 29, 31, and 32, which are all of the claims pending in this application.

Appellants' invention relates to a program data distribution method in which an identification code is transmitted with the program data to the terminal and is used to obtain the decryption key from a key server. Claims 10 and 11 are illustrative of the claimed invention and read as follows:

10. A terminal comprising:

control means for processing encrypted program data transmitted by a file server connected to an open network;

a first memory for storing program data that is distributed by said file server and that is decoded by using a decryption key, which is transmitted from a key server connected to the open network; and

a second memory for storing a serial code;

before said program data that is decoded is stored in said first memory, said control means encrypting said program data by using the serial code stored in the second memory, and before said program data is read from said first memory, said control means decoding said program data by using said serial code.

11. A program data distribution method for use with an open network comprising the steps of:

issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key;

distributing program data encrypted by the encryption key from a file server connected to said open network;

distributing a decryption key from a key server connected to said open network, said decryption key used to decode said encrypted program data; and

employing said decryption key distributed by said key server to decode said encrypted program data obtained from said file server by a terminal, which is connected to said open network for processing program data,

wherein, at the step of distributing encrypted data, the identification code is transmitted along with the program data to the terminal, the terminal transmits the received identification code to the key server, and based on the identification code, the key server searches for a decryption key used to decrypt the program data and transmits the decryption key to the terminal.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

McCarty	5,666,411	Sep. 09, 1997 (filed Jan. 13, 1994)
Erickson	5,765,152	June 09, 1998 (filed Oct. 13, 1995)
Wasilewski et al. (Wasilewski)	5,870,474	Feb. 09, 1999 (filed Dec. 29, 1995)
Allen	5,909,638	June 01, 1999 (filed Aug. 06, 1996)
Steinberg et al. (Steinberg)	6,000,030	Dec. 07, 1999 (filed June 20, 1996)

Claims 4 through 11, 13, 15 through 22, 25, 27, 29, 31, and 32 stand rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Wasilewski, McCarty, and Allen.

Claims 5, 6, 16 through 18, and 25 stand rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Wasilewski and Erickson.

Claims 8, 9, 20, 21, 29, and 31 stand rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Wasilewski.

Reference is made to the Examiner's Answer (Paper No. 23, mailed December 20, 2001) for the examiner's complete reasoning in support of the rejections, and to appellants' Brief (Paper No. 22, filed October 26, 2001) and Reply Brief (Paper No. 24, filed February 20, 2002) for appellants' arguments thereagainst.

OPINION

We have carefully considered the claims, the applied prior art references, and the respective positions articulated by appellants and the examiner. As a consequence of our review, we will reverse the obviousness rejections of claims 4 through 11, 13, 15 through 22, 25, 27, 29, 31, and 32.

Each of claims 10, 11, 13, 22, and 32, the independent claims, recites decoding using a decryption key transmitted or distributed from a key server. The examiner states (Answer, page 4) that Steinberg "is vague in disclosing 'a key server independent from the file server, for distributing the decryption key issued by the manager.'" Steinberg, however, is quite clear that the decryption key is selected, not received, by the user (see column 3, lines 37-41). Nonetheless, the examiner attempts to cure the deficiency of Steinberg with Wasilewski, pointing out that Wasilewski includes a public key server. Yet, nowhere in the rejection does the examiner explain the motivation for modifying Steinberg to include a key server as disclosed by Wasilewski. The examiner asserts (Answer, page 5) that combining the systems of Steinberg, Wasilewski, McCarty and Allen yields a number of supposed benefits. This, however, does not explain the motivation for each specific modification nor exactly how one would modify the primary reference to satisfy all of the claim limitations.

In response to appellants' argument that Steinberg fails to teach a decryption key distributed by a key server, the examiner states (Answer, pages 11-12) that the difference between Steinberg and appellants' system, the supplier of the identification code and encryption key,

> is superficial, as the appellant's [sic] invention does not define a systematic process that would enable one of ordinary skill of the art to distinguish a user supplied versus a server supplied identification code and key. Moreover, there are many ways a user can obtain an encryption (or decryption) key, therefore, it would have been obvious to use the EXCHANGE network of McCarty to request a key . . . to provide further security to the end-user's system. The advantage being that an attack that compromises a system that uses a single user encryption/ decryption key pair . . . to encrypt requested software, allows the attacker access to the entire user library of requested software, whereas in a system that uses multiple encryption keys to encrypt data including a key that is specific to the requested program, or software, would only allow the attacker, to at best, a single program.

There are numerous problems with the examiner's reasoning. First, appellants do define a process that distinguishes a user supplied versus a server supplied identification code and key. Specifically, appellants disclose (Specification, page 7, line 20-page 8, line 4) and claim that the user obtains a program file and an ID number that corresponds to the program file from the file server. The user transmits the received ID number to the key server. The key server uses the ID number to find the corresponding decryption key and transmits the key to the user's terminal. Clearly, as disclosed and claimed, the identification code originates at the file server and the decryption key originates at a key server and each is received by the user. The user is not the source of either the identification code or the key; servers supply both.

Next, that a user "can" obtain an encryption key different ways does not speak to the obviousness of obtaining the key a different way. The Federal Circuit has held that "[t]he mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification." ***In re Fritch***, 972 F.2d 1260, 1266 n.14, 23 USPQ2d 1780, 1783-4 n.14 (Fed. Cir. 1992), ***citing In re Gordon***, 733 F.2d 900, 902, 221, USPQ 1125, 1127 (Fed. Cir. 1984).

Further, we are unable to find in the references the advantages given by the examiner for the modification. A factual inquiry whether to modify a reference must be based on objective evidence of record, not merely conclusionary statements of the examiner. ***See In re Lee***, 277 F.2d 1338, 1342-43, 61 USPQ2d 1430, 1433 (Fed. Cir. 2002). Also, adding to Steinberg's system a key server for distributing the decryption key would involve a complete redesign of the system rather than a modification, as suggested by the examiner.

The examiner asserts (Answer, page 12) that Steinberg is not limited to the user's defining the encryption key, but rather, also includes an embodiment in which encryption is performed "with or without the user encryption key." The examiner concludes (Answer, pages 12-13) that it would have been obvious "in the spirit of Steinberg . . . to encrypt the software with a program key and authorized user computer system key." As pointed out by appellants (Reply Brief, page 3), in the alternative embodiment referenced by the examiner, the encryption key is derived at least in part from the address at which the program exists on the disk drive and then remains in the file server. At no point is the key distributed to the user or terminal. Therefore, as asserted by appellants (Reply Brief, page 4) "there is no reason for the user to receive a key from any key server," and the examiner has not provided any compelling reason for such.

As stated ***supra***, Steinberg fails to disclose a key server for supplying the decryption key, and neither Wasilewski nor McCarty suggests modifying Steinberg to include the claimed key server. Further, Allen fails to cure the shortcomings of the other references. Consequently, we cannot sustain the obviousness rejection of independent claims 10, 11, 13, 22, and

32 over Steinberg, Wasilewski, McCarty, and Allen, nor of their dependents, claims 4 through 9, 15 through 21, 25, 27, 29, and 31.

Regarding the rejection of claims 5, 6, 16 through 18, and 25 over Steinberg, Wasilewski, and Erickson, we note first that a procedural error exists in that the rejected claims are dependent claims whose independent claims were not rejected over the same or a subset of the same references. As dependent claims include all of the limitations of the claims from which they depend, if the references satisfy the dependent claims, they must also satisfy the independent claims from which they depend. Going to the merits of the rejection, we cannot sustain the rejection over Steinberg, Wasilewski, and Erickson because Steinberg and Wasilewski fail to disclose the claimed key server, as explained ***supra***, and Erickson fails to cure this deficiency. Accordingly, we will reverse the rejection of claims 5, 6, 16 through 18, and 25 over Steinberg, Wasilewski, and Erickson.

Similarly, dependent claims 8, 9, 20, 21, 29, and 31 should not have been rejected over Steinberg and Wasilewski if the independent claims are not considered to be satisfied by the two references. As to the merits of the rejection, as previously discussed, since Steinberg and Wasilewski fail to disclose the claimed key, we cannot sustain the obviousness rejection of claims 8, 9, 20, 21, 29, and 31.

CONCLUSION

The decision of the examiner rejecting claims 4 through 11, 13, 15 through 22, 25, 27, 29, 31, and 32 under 35 U.S.C. § 103 is reversed.

REVERSED

KENNETH W. HAIRSTON)
Administrative Patent Judge)
)
)
)
) BOARD OF PATENT
ERROL A. KRASS) APPEALS
Administrative Patent Judge) AND
) INTERFERENCES
)
)
)
ANITA PELLMAN GROSS)
Administrative Patent Judge)

DICKSTEIN SHAPIRO MORIN & OSHINSKY
2101 L STREET NW
WASHINGTON, DC 20037